

**IN THE CLAIMS:**

- 1 1. (original) A method of proving entity membership in a nested group, wherein a  
2 presenter of credentials performs the step of presenting to a recipient of credentials one or  
3 more chains of group credentials.
- 13 1 2. (original) The method of claim 1, wherein one of said chains of group credentials  
2 comprise one or more proofs of group membership.
- 1 3. (original) The method of claim 2, wherein said proofs of group membership  
2 comprise one or more group membership certificates.
- 1 4. (original) The method of claim 2, wherein said proofs of group membership  
2 comprise one or more group membership lists.
- 1 5. (original) The method of claim 1, wherein one of said chains of group credentials  
2 comprise one or more proofs of group non-membership.
- 1 6. (original) The method of claim 5, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.
- 1 7. (original) The method of claim 5, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.
- 1 8. (original) The method of claim 1, wherein said recipient is a resource server.
- 1 9. (original) The method of claim 1, wherein said recipient is an on-line group  
2 server.

1 10. (original) The method of claim 1, wherein said recipient is an on-line revocation  
2 server.

1 11. (original) The method of claim 1, wherein said recipient is a client.

1 12. (original) A method of proving entity non-membership in a nested group,  
2 wherein a presenter of credentials performs the step of presenting to a recipient of cre-  
3 dentials one or more chains of group credentials.

1 13. (original) The method of claim 12, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 14. (original) The method of claim 13, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 15. (original) The method of claim 13, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 16. (original) The method of claim 12, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 17. (original) The method of claim 16, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 18. (original) The method of claim 16, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 19. (original) The method of claim 12, wherein said recipient is a resource server.

1 20. (original) The method of claim 12, wherein said recipient is an on-line group  
2 server.

1 21. (original) The method of claim 12, wherein said recipient is an on-line revocation  
2 server.

1 22. (original) The method of claim 12, wherein said recipient is a client.

1 23. (original) A computer system wherein a presenter of credentials presents to a re-  
2 cipient of credentials one or more chains of group credentials to prove entity membership  
3 in a nested group.

1 24. (original) The system of claim 23, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 25. (original) The system of claim 24, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 26. (original) The system of claim 24, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 27. (original) The system of claim 23, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 28. (original) The system of claim 27, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 29. (original) The system of claim 27, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 30. (original) The system of claim 23, wherein said recipient is a resource server.

1 31. (original) The system of claim 23, wherein said recipient is an on-line group  
2 server.

1 32. (original) The system of claim 23, wherein said recipient is an on-line revocation  
2 server.

1 33. (original) The system of claim 23, wherein said recipient is a client.

1 34. (original) A computer system wherein a presenter of credentials presents to a re-  
2 cipient of credentials one or more chains of group credentials to prove entity non-  
3 membership in a nested group.

1 35. (original) The system of claim 34, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 36. (original) The system of claim 35, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 37. (original) The system of claim 35, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 38. (original) The system of claim 34, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 39. (original) The system of claim 38, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 40. (original) The system of claim 38, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 41. (original) The system of claim 34, wherein said recipient is a resource server.

1 42. (original) The system of claim 34, wherein said recipient is an on-line group  
2 server.

1 43. (original) The system of claim 34, wherein said recipient is an on-line revocation  
2 server.

1 44. (original) The system of claim 34, wherein said recipient is a client.

1 45. (original) A method of operating a client device on a computer network, said cli-  
2 ent device requesting a service from a server and performing the steps of:

3 A. obtaining one or more chains of group credentials to prove client membership  
4 in a nested group, and

5 B. presenting to the server a request for the service, said request including the  
6 chains of group credentials.

1 46. (original) The method of claim 45, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 47. (original) The method of claim 46, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 48. (original) The method of claim 46, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 49. (original) The method of claim 45, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 50. (original) The method of claim 49, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 51. (original) The method of claim 49, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 52. (original) A method of operating a client device on a computer network, said cli-  
2 ent device requesting a service from a server and performing the steps of:

3 A. obtaining one or more chains of group credentials to prove client non-  
4 membership in a nested group, and

5 B. presenting to the server a request for the service, said request including the  
6 chains of group credentials.

1 53. (original) The method of claim 52, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 54. (original) The method of claim 53, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 55. (original) The method of claim 53, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 56. (original) The method of claim 52, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 57. (original) The method of claim 56, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 58. (original) The method of claim 56, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 59. (original) A client device on a computer network requesting a service from a  
2 server, said client device comprising:

3 A. means for obtaining one or more chains of group credentials to prove client  
4 membership in a nested group, and

5 B. means for presenting to the server a request for the service, said request in-  
6 cluding the chains of group credentials.

1 60. (original) The client device of claim 59, wherein one of said chains of group cre-  
2 dentials comprise one or more proofs of group membership.

1 61. (original) The client device of claim 60, wherein said proofs of group member-  
2 ship comprise one or more group membership certificates.

1 62. (original) The client device of claim 60, wherein said proofs of group member-  
2 ship comprise one or more group membership lists.

1 63. (original) The client device of claim 59, wherein one of said chains of group cre-  
2 dentials comprise one or more proofs of group non-membership.

1 64. (original) The client device of claim 63, wherein said proofs of group non-  
2 membership comprise one or more group non-membership certificates.

1 65. (original) The client device of claim 63, wherein said proofs of group non-  
2 membership comprise one or more group membership lists.

1 66. (original) A client device on a computer network requesting a service from a  
2 server, said client device comprising:

3 A. means for obtaining one or more chains of group credentials to prove client  
4 non-membership in a nested group, and

5 B. means for presenting to the server a request for the service, said request in-  
6 cluding the chains of group credentials.

1 67. (original) The client device of claim 66, wherein one of said chains of group cre-  
2 dentials comprise one or more proofs of group membership.

1 68. (original) The client device of claim 67, wherein said proofs of group member-  
2 ship comprise one or more group membership certificates.

1 69. (original) The client device of claim 67, wherein said proofs of group member-  
2 ship comprise one or more group membership lists.

1 70. (original) The client device of claim 66, wherein one of said chains of group cre-  
2 dentials comprise one or more proofs of group non-membership.

1 71. (original) The client device of claim 70, wherein said proofs of group non-  
2 membership comprise one or more group non-membership certificates.



1 72. (original) The client device of claim 70, wherein said proofs of group non-  
2 membership comprise one or more group membership lists.

1 73. (original) A method for operating a resource server on a computer network, said  
2 resource server controlling access to one or more resources by a plurality of client de-  
3 vices and performing the steps of:

4 A. accepting resource access requests from the client devices, each request com-  
5 prising one or more chains of group credentials proving client membership in a nested  
6 group,

7 B. validating the chains of group credentials, and

8 C. if the chains of group credentials are valid, authorizing the requested access.

1 74. (original) The method of claim 73, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 75. (original) The method of claim 74, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 76. (original) The method of claim 74, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 77. (original) The method of claim 73, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 78. (original) The method of claim 77, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 79. (original) The method of claim 77, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 80. (original) A method of operating a resource server on a computer network, said  
2 resource server controlling access to one or more resources by a plurality of client de-  
3 vices and performing the steps of:

4 A. accepting resource access requests from the client devices, each request com-  
5 prising one or more chains of group credentials proving client non-membership in a  
6 nested group,

7 B. validating the chains of group credentials, and

8 C. if the chains of group credentials are valid, authorizing the requested access.

1 81. (original) The method of claim 80, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group membership.

1 82. (original) The method of claim 81, wherein said proofs of group membership  
2 comprise one or more group membership certificates.

1 83. (original) The method of claim 81, wherein said proofs of group membership  
2 comprise one or more group membership lists.

1 84. (original) The method of claim 80, wherein one of said chains of group creden-  
2 tials comprise one or more proofs of group non-membership.

1 85. (original) The method of claim 84, wherein said proofs of group non-membership  
2 comprise one or more group non-membership certificates.

1 86. (original) The method of claim 84, wherein said proofs of group non-membership  
2 comprise one or more group membership lists.

1 87. (original) A resource server on a computer network controlling access to one or  
2 more resources by a plurality of client devices, said resource server comprising:

3 A. means for accepting resource access requests from the client devices, each re-  
4 quest comprising one or more chains of group credentials proving client membership in a  
5 nested group,

6 B. means for validating the chains of group credentials, and

7 C. if the chains of group credentials are valid, means for authorizing the re-  
8 quested access.

1 88. (original) The resource server of claim 87, wherein one of said chains of group  
2 credentials comprise one or more proofs of group membership.

1 89. (original) The resource server of claim 88, wherein said proofs of group member-  
2 ship comprise one or more group membership certificates.

1 90. (original) The resource server of claim 88, wherein said proofs of group member-  
2 ship comprise one or more group membership lists.

1 91. (original) The resource server of claim 87, wherein one of said chains of group  
2 credentials comprise one or more proofs of group non-membership.

1 92. (original) The resource server of claim 91, wherein said proofs of group non-  
2 membership comprise one or more group non-membership certificates.

1 93. (original) The resource server of claim 91, wherein said proofs of group non-  
2 membership comprise one or more group membership lists.

1 94. (original) A resource server on a computer network controlling access to one or  
2 more resources by a plurality of client devices, said resource server comprising:

3 A. means for accepting resource access requests from the client devices, each re-  
4 quest comprising one or more chains of group credentials proving client non-membership  
5 in a nested group,

6 B. means for validating the chains of group credentials, and

7 C. if the chains of group credentials are valid, means for authorizing the re-  
8 quested access.

1 95. (original) The resource server of claim 94, wherein one of said chains of group  
2 credentials comprise one or more proofs of group membership.

1 96. (original) The resource server of claim 95, wherein said proofs of group member-  
2 ship comprise one or more group membership certificates.

1 97. (original) The resource server of claim 95, wherein said proofs of group member-  
2 ship comprise one or more group membership lists.

1 98. (original) The resource server of claim 94, wherein one of said chains of group  
2 credentials comprise one or more proofs of group non-membership.

1 99. (original) The resource server of claim 98, wherein said proofs of group non-  
2 membership comprise one or more group non-membership certificates.

1 100. (original) The resource server of claim 98, wherein said proofs of group non-  
2 membership comprise one or more group membership lists.

1 101. (original) A computer data signal embodied in a carrier wave and representing a  
2 sequence of instructions that, when executed by a processor in a network device request-  
3 ing a service from a server, configures the network device to operate as a client device  
4 that:

5 A. obtains one or more chains of group credentials to prove client membership in  
6 a nested group, and

7 B. presents to the server a request for the service, said request including the  
8 chains of group credentials.

1 102. (original) The computer data signal of claim 101, wherein one of said chains of  
2 group credentials comprise one or more proofs of group membership.

1 103. (original) The computer data signal of claim 102, wherein said proofs of group  
2 membership comprise one or more group membership certificates.

1 104. (original) The computer data signal of claim 102, wherein said proofs of group  
2 membership comprise one or more group membership lists.

1 105. (original) The computer data signal of claim 101, wherein one of said chains of  
2 group credentials comprise one or more proofs of group non-membership.

1 106. (original) The computer data signal of claim 105, wherein said proofs of group  
2 non-membership comprise one or more group non-membership certificates.

1 107. (original) The computer data signal of claim 105, wherein said proofs of group  
2 non-membership comprise one or more group membership lists.

1 108. (original) A computer data signal embodied in a carrier wave and representing a  
2 sequence of instructions that, when executed by a processor in a network device request-  
3 ing a service from a server, configures the network device to operate as a client device  
4 that:

5 A. obtains one or more chains of group credentials to prove client non-  
6 membership in a nested group, and

7 B. presents to the server a request for the service, said request including the  
8 chains of group credentials.

1 109. (original) The computer data signal of claim 108, wherein one of said chains of  
2 group credentials comprise one or more proofs of group membership.

1 110. (original) The computer data signal of claim 109, wherein said proofs of group  
2 membership comprise one or more group membership certificates.

1 111. (original) The computer data signal of claim 109, wherein said proofs of group  
2 membership comprise one or more group membership lists.

1 112. (original) The computer data signal of claim 108, wherein one of said chains of  
2 group credentials comprise one or more proofs of group non-membership.

1 113. (original) The computer data signal of claim 112, wherein said proofs of group  
2 non-membership comprise one or more group non-membership certificates.

1 114. (original) The computer data signal of claim 112, wherein said proofs of group  
2 non-membership comprise one or more group membership lists.

1 115. (original) A computer data signal embodied in a carrier wave and representing a  
2 sequence of instructions that, when executed by a processor in a network device control-  
3 ling access to one or more resources by a plurality of client devices, configures the net-  
4 work device to operate as a resource server that:

5 A. accepts resource access requests from the client devices, each request com-  
6 prising one or more chains of group credentials proving client membership in a nested  
7 group,

8 B. validates the chains of group credentials, and

9 C. if the chains of group credentials are valid, authorizes the requested access.

1 116. (original) The computer data signal of claim 115, wherein one of said chains of  
2 group credentials comprise one or more proofs of group membership.

1 117. (original) The computer data signal of claim 116, wherein said proofs of group  
2 membership comprise one or more group membership certificates.

1 118. (original) The computer data signal of claim 116, wherein said proofs of group  
2 membership comprise one or more group membership lists.

1 119. (original) The computer data signal of claim 115, wherein one of said chains of  
2 group credentials comprise one or more proofs of group non-membership.

1 120. (original) The computer data signal of claim 119, wherein said proofs of group  
2 non-membership comprise one or more group non-membership certificates.

1 121. (original) The computer data signal of claim 119, wherein said proofs of group  
2 non-membership comprise one or more group membership lists.

1 122. (original) A computer data signal embodied in a carrier wave and representing a  
2 sequence of instructions that, when executed by a processor in a network device control-  
3 ling access to one or more resources by a plurality of client devices, configures the net-  
4 work device to operate as a resource server that:

5 A. accepts resource access requests from the client devices, each request com-  
6 prising one or more chains of group credentials proving client non-membership in a  
7 nested group,

8 B. validates the chains of group credentials, and

9 C. if the chains of group credentials are valid, authorizes the requested access.

1 123. (original) The computer data signal of claim 122, wherein one of said chains of  
2 group credentials comprise one or more proofs of group membership.

1 124. (original) The computer data signal of claim 123, wherein said proofs of group  
2 membership comprise one or more group membership certificates.

1 125. (original) The computer data signal of claim 123, wherein said proofs of group  
2 membership comprise one or more group membership lists.

1 126. (original) The computer data signal of claim 122, wherein one of said chains of  
2 group credentials comprise one or more proofs of group non-membership.

1 127. (original) The computer data signal of claim 126, wherein said proofs of group  
2 non-membership comprise one or more group non-membership certificates.

1 128. (original) The computer data signal of claim 126, wherein said proofs of group  
2 non-membership comprise one or more group membership lists.